Rijkswaterstaat
Ministerie van Infrastructuur en Milieu

RWS ONGECLASSIFICEERD

Verwerking van afgedankte datadragende ICT hardware binnen de Rijksoverheid

Deze rapportage beschrijft de uitkomsten van het onderzoek naar de verwerking van afgedankte, datadragende ict-apparatuur binnen de Rijksoverheid.

Datum	19 januari 2015
Status	Definitief

Colofon

Uitgegeven door	Rijkswaterstaat
Uitgevoerd door	Water, Verkeer en Leefomgeving
Datum	19 januari 2015
Status	Definitief

Inhoud

Managementsamenvatting

Binnen de rijksoverheid worden jaarlijks circa 30.000 stuks datadragende ict-apparatuur overtollig gesteld. De verantwoordelijk gestelde organisatie binnen de rijksoverheid, Domeinen Roerende Zaken, heeft in het verleden op basis van dataveiligheid, kosten en milieu ervoor gekozen deze apparatuur te vernietigen middels een shredder, en de scrap zo optimaal mogelijk af te zetten.

In dit onderzoek is inzichtelijk gemaakt welke alternatieven er zijn binnen de kaders van de rijksoverheid voor het verwerken van overtollige datadragende ict-apparatuur, rekening houdend met de veranderende technologieën, kosten, en aandacht voor het milieu (circulaire economie). Daartoe zijn wet- en regelgeving, hoeveelheden en soorten apparatuur in kaart gebracht. Vervolgens zijn via gesprekken met betrokkenen de huidige praktijk en de randvoorwaarden beschreven. Indicatief zijn een aantal verwerkingsroutes opgenomen, die via een marktverkenning concreet zijn uitgewerkt. Op basis hiervan is een voorstel tot stand gekomen.

De verwerking van overtollige ict-apparatuur binnen de rijksoverheid is vastgelegd in de Regeling Materieelbeheer. Deze regeling is niet overal binnen de rijksoverheid bekend, of wordt in elk geval niet altijd nageleefd. Diverse overheidspartijen geven aan te kiezen voor alternatieven, met name op basis van ontzorging en kosten. Een aantal alternatieve verwerkingsroutes zijn onderzocht middels een marktconsultatie. Gebleken is daarbij dat een groot deel van de datadragende ict-apparatuur gecertificeerd kan worden geschoond en vervolgens hergebruikt, dat dit tegen minder kosten of zelfs opbrengst mogelijk is, en dat alternatieven beter scoren op het aspect milieu. Geadviseerd wordt om apparatuur waarop informatie is verwerkt met de rubriceringen "Stg. Geheim" en "Stg. Zeer Geheim" (maximaal 5% van het totale aanbod) blijvend te vernietigen middels een shredder om hiervoor volledige dataveiligheid blijvend te garanderen.

Op basis van de resultaten van het onderzoek zal een Europese aanbesteding voor de verwerking van overtollige, datadragende gecertificeerd schoonbare ict-apparatuur binnen de rijksoverheid tot het rubriceringsniveau "Stg. Geheim" worden gestart. De huidige verwerker, Domeinen Roerende Zaken, blijft in dit proces conform de regeling Materieelbeheer een centrale rol spelen: Domeinen schoont de ict-apparatuur en zorgt daarna voor afvoer naar de markt. De in de rapportage benoemde randvoorwaarden worden zo uitgewerkt dat deze ook juridisch kunnen worden gebruikt voor een Europese aanbesteding. Zo kan een toekomstbestendige verwerkingsroute worden verzekerd, waarin dataveiligheid is gegarandeerd, die financieel voor de Rijksoverheid aantrekkelijk is en past in het streven naar een circulaire economie.

Projectdoelstellingen

Doel van het project is om in kaart te brengen hoe binnen de kaders van de rijksoverheid het afstoten en/of de vernietiging van overtollige datadragers (hardware) zo optimaal mogelijk kan worden vormgegeven. Deze doelstelling is opgesplitst in de volgende onderzoeksvragen:

a. Welke alternatieve verwerkingsmethoden voor de datadragende ICT hardware van de rijksoverheid zijn beschikbaar en realistisch (randvoorwaarde: data moet worden gewist)?
b. Hoe verhouden de potentiële gevolgen van deze alternatieven zich ten opzichte van de huidige werkwijze (onder andere financieel, logistiek en milieutechnisch)?
c. Welke beveiligings-, technische, juridische en contractuele randvoorwaarden kunnen worden aangepast om optimale verwerking van ICT hardware mogelijk te maken.

Eén of meerdere opties worden voorzien van een businesscase en ter advisering voorgelegd aan de stuurgroep.

1 Uitgangspunten Onderzoek

Het onderzoek richt zich alleen op afgedankte, datadragende ict-apparatuur (verder: ict-apparatuur) binnen de Rijksoverheid. Daarnaast is van belang dat eventuele alternatieve verwerkingsroutes voldoen aan een drietal randvoorwaarden:

- De kosten van de alternatieven dienen niet hoger te zijn dan de huidige verwerkingsroute;
- Dataveiligheid dient te zijn gewaarborgd;
- Milieuaspecten dienen bij de alternatieven in kaart te zijn gebracht en indien mogelijk worden vergeleken met de huidige verwerkingsroute.

1.1 Rijksoverheid

Binnen de Rijksoverheid vallen de ministeries met de daaronder ressorterende diensten, bedrijven en instellingen. Een aparte plaats wordt ingenomen door het ministerie van Defensie en de AIVD en MIVD, die vanwege de gevoeligheid van hun informatie een aparte plaats innemen en op dit moment zorgdragen voor hun eigen afdanking en verwerking van ict-apparatuur.
Eind 2012 waren er circa 116.500 mensen (circa 109.000 fte) werkzaam binnen de sector Rijk (bron http://www.kosmos-kennisbank.nl/tabellen-grafieken), exclusief Defensie (ca. 60.000 fte).

1.2 Apparatuur

De scope van het onderzoek, datadragende ict-apparatuur, is tweeledig: ict(werkplek)-apparatuur (pc's, servers, laptops, tablets, printers etc.) en (mobiele) datadragers (disks, usb-sticks, CD's, DVD's, etc.). Voor de werkplekapparatuur wordt gerekend met een vervangingstermijn van 3 jaar. Met name servers en printers worden echter vaak langer gebruikt vanwege compatibiliteit van programma's. Voor overige, met name draagbare, apparatuur is geen vaste vervangingstermijn vastgelegd.
De rapportage richt zich met name op de verwerking van de ict-apparatuur. Voor de datadragers is contractueel een aparte inzamelings- en verwerkingsroute vastgelegd via categoriemanagement papier, drukwerk en afvoer vertrouwelijk papier.

1.3 Wet- en regelgeving (Ict-apparatuur)

De huidige verwerkingsroute van ict-apparatuur is beschreven in de regeling materieelbeheer (Ministerie van Financiën, 2006). Daarbij is afvoer via Domeinen Roerende Zaken, onderdeel van het ministerie van Financiën, beschreven als vastgestelde route.
Naast deze regeling zijn nog een aantal andere regels direct van invloed op de verwerking van ict-apparatuur: de organisatie, verantwoordelijkheden en regels rond beveiliging en beveiligingsprocedures van informatie en ict-apparatuur zijn vastgelegd in het Beveiligingsvoorschrift 2013, het Besluit voorschrift informatiebeveiliging rijksdienst (Vir, Ministerie van Algemene Zaken, 2007) en het Besluit voorschrift informatiebeveiliging rijksdienst – bijzondere informatie (Vir-bi, Ministerie van Algemene Zaken, 2013). Elke individuele ambtenaar wordt geacht zich aan de, voor hem van toepassing zijnde, voorschriften te houden.

De Regeling materieelbeheer (Ministerie van Financiën, 2006) is met name van belang voor de procedure voor afstoting van roerende zaken, waaronder ict-apparatuur.
De verschillende regelgevingen zijn hieronder nader toegelicht.

A. Beveiligingsvoorschrift rijksdienst (Ministerie van Algemene Zaken, 2013)
Dit voorschrift behelst binnen de Rijksoverheid de integrale beveiliging: het selecteren, implementeren en periodiek evalueren van een samenhangend stelsel van onder meer informatiesystemen op basis van risicomanagement. In dit voorschrift worden met name de functionarissen benoemd die een rol spelen in de beveiliging: rijksbeveiligingsambtenaar, departementale secretaris-generaal, departementale beveiligingsambtenaar (dep BVA) en de lijnmanager. Tijdens het onderzoek is gebleken dat binnen de departementen ook de CIO (Chief information officer) en de CISO (Chief information security officer) een rol spelen.

B. Besluit Voorschriften informatiebeveiliging rijksdienst (Vir 2007)
Dit Besluit heeft betrekking op het hele proces van informatie en de hele levenscyclus van informatiesystemen, inclusief daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie, binnen de Rijksoverheid. De secretaris-generaal van een Ministerie stelt het informatiebeveiligingsbeleid vast, draagt dit uit en legt verantwoording hierover af. Het lijnmanagement is verantwoordelijk voor de beveiliging van zijn informatiesystemen.

C. Besluit Voorschriften informatiebeveiliging rijksdienst – bijzondere informatie (Vir-bi 2013)
Het Besluit Vir-bi gaat specifiek in op de beveiliging van bijzondere informatie, en geldt als aanvulling op het Vir. Bijzondere informatie is informatie die gerubriceerd is onder één van de niveaus Zeer geheim, Geheim, Confidentieel of Departementaal Vertrouwelijk. Kennisname door niet geautoriseerden kan nadelige gevolgen hebben voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries.
De maatregelen voor beveiliging van bijzondere informatie worden onder de verantwoordelijkheid van de BVA of de accreditatieautoriteit (Geheim, Zeer Geheim) periodiek gecontroleerd. Alle bedrijfsmiddelen waarop bijzondere informatie wordt verwerkt en de personen aan wie ze zijn uitgereikt moeten worden geregistreerd, evenals de locatie/standplaats van alle middelen en de toewijzing aan een eigenaar. Voorafgaand aan verwerving, ontwikkeling, onderhoud en afstoot van informatiesystemen waarin bijzondere informatie wordt verwerkt, dienen de dreigingen en risico's in beeld te zijn gebracht (bij Geheim en Zeer Geheim door een onafhankelijk deskundige).

D. Baseline Informatiebeveiliging Rijksdienst (BIR)
Naast de VIR beschikt(e) ieder ministerie ook over een eigen baseline. Door de toename van gegevensuitwisseling tussen ministeries is echter behoefte ontstaan aan een meer uitgebreide rijksbrede baseline. De Baseline Informatiebeveiliging Rijksdienst (BIR) vervangt alle departementale en interdepartementale baselines op gebied van informatiebeveiliging. Het beoogde niveau van de baseline is "departementaal vertrouwelijk en Wet Bescherming Persoonsgegevens risicoklasse II". De baseline omvat een verplicht tactisch normenkader (BIR-TNK) en een ondersteunende operationele baseline (BIR-OB) die een groot deel van het tactisch kader dekt.

E. Regeling materieelbeheer (2006)
In artikel 8 van deze regeling wordt specifiek ingegaan op afstoting van roerende zaken.

Artikel 8
1. De minister of het college neemt over roerende zaken die niet langer nodig zijn voor de bedrijfsvoering van zijn ministerie, respectievelijk van het college zo spoedig mogelijk een besluit tot overtolligstelling.
2. De minister of het college doet van een besluit tot overtolligstelling zo spoedig mogelijk mededeling aan de dienst Domeinen.
3. De minister of het college draagt overtollig gestelde, roerende zaken in tijdelijk beheer over aan de dienst Domeinen, tenzij het zaken betreft die door middel van inruil worden verkocht.
4. De overdracht in tijdelijk beheer aan de dienst Domeinen geschiedt na acceptatie door de dienst Domeinen en met inachtneming van gemaakte budgettairemiddelenafspraken dan wel van gemaakte budgettairebijdrageafspraken.
5. De dienst Domeinen draagt het materieelbeheer van overtollig gestelde zaken via ingebruikgeving aan andere ministers of colleges of via verhuur aan derden over, dan wel stoot die zaken via verkoop aan derden af. Verhuur of verkoop aan derden geschiedt tegen marktconforme prijzen.
6. De dienst Domeinen kan de kosten van afstoting geheel of gedeeltelijk aan de overtolligstellende minister of het college in rekening brengen, indien zij die kosten niet kan dekken uit de opbrengst van afstoting. Zij doet daarvan zo spoedig mogelijk mededeling aan de minister of het college.
7. De dienst Domeinen kan toestemming verlenen dat afstoting door de minister of het college zelf plaatsvindt. Aan die toestemming kunnen voorwaarden worden verbonden.
8. Roerende zaken die niet op de in het vijfde lid bedoelde wijze kunnen worden afgestoten of overgedragen, stoot de dienst Domeinen voor rekening van de minister of het college door middel van vernietiging af.
9. Indien naar het oordeel van de dienst Domeinen de minister of het college een besluit tot overtolligstelling of een overdracht in tijdelijk beheer aan de dienst Domeinen ondoelmatig lang uitstelt, kan de dienst Domeinen, nadat de Minister van Financiën de minister of het college schriftelijk een voorstel tot overdracht in tijdelijk beheer heeft gedaan, de betrokken zaak zonder een besluit tot overtolligstelling in tijdelijk beheer overnemen.

Hoofdlijn uit deze regeling is dat bij overtolligstelling Domeinen altijd op de hoogte wordt gesteld, dat Domeinen na beoordeling van de risico's (milieu, informatie) de verdere bestemming bepaalt en de financiële afhandeling marktconform verzorgt. De verantwoordelijkheid voor de gevolgen van dergelijke risico's berust bij de overdragende dienst, tenzij Domeinen die verantwoordelijkheid expliciet heeft overgenomen. In de Ministerraad van 1 december 2000 is besloten Domeinen verantwoordelijk te stellen voor het schonen van computers. Dit betekent dat alle computers die aan Domeinen worden aangeboden, onder verantwoordelijkheid van Domeinen worden geschoond. Bij schenkingen of inruil van computers, die niet via Domeinen verlopen, biedt Domeinen facilitaire ondersteuning bij de schoning. Domeinen kan (eventueel onder voorwaarden) conform de toelichting bij de regeling materieelbeheer ook toestemming verlenen voor andersoortige afstoting door de ontdoener zelf.

Achterliggende gedachte is dat de expertise van Domeinen van belang is om overtollige zaken met een nog resterende economische levensduur of economische waarde na beoordeling van risico's tegen marktconforme prijzen en veilig te gelde te maken.

2 Huidige praktijk

In dit hoofdstuk zijn de bevindingen opgenomen van het onderzoek op basis van gesprekken en research. Contacten zijn geraadpleegd bij Domeinen, ministerie van BZK, ministerie van IenM, ministerie van VenJ, de AIVD, het Shared Service Centre Ict (SSC-Ict) en Blancco (leverancier van gecertificeerde software voor informatievernietiging). Ook is overleg gevoerd met de Rijksbeveiligingsambtenaar.

2.1 Verwerkingsroute

Ict-apparatuur
Zoals hierboven aangegeven is in de regeling materieelbeheer een verwerkingsroute voorgeschreven via Domeinen. Met ingang van 1 juli 2010 verkoopt Domeinen geen geschoonde desk- en/of laptops meer, maar vult zijn verantwoordelijkheid voor de verwerking van ict-apparatuur in door deze te vernietigen middels een shredder. De motivatie van deze verwerking is te vinden op een informatieblad via de website van Domeinen.

Speerpunt rijksoverheid
Informatie van de (rijks)overheid mag niet op straat terecht komen. Informatie via welk middel dan ook. Op papier of digitaal. Digitale datadragers kennen we in verschillende vormen; mobiele telefoons, harde schijven uit desk- en laptops, servers, printers en ook faxen.

- Voorkomen moet worden dat desk- en laptops worden verkocht aan handelaren die deze verschepen naar derde wereld landen. Het gevaar bestaat dan dat de computerapparatuur alsnog en ongecontroleerd in het afvalcircuit terechtkomt;
- De techniek staat niet stil. De technische ontwikkeling met betrekking tot de dichtheid (density) van harde schijven gaat snel en maakt deze schijven compacter. Hierdoor wordt het moeilijker de schijven via dataverwijderingssoftware 100% te schonen. Daarnaast wordt deze software steeds duurder. Ook vergt het beoordelen en screenen hiervan meer kennis, capaciteit en tijd waardoor het wordt bemoeilijkt tijdig de laatste dataverwijderingssoftware te laten screenen. Het gevaar bestaat dat de data dus onvoldoende geschoond wordt;
- Door de bezuinigingen neemt de economische levensduur (gebruik) van de hardware toe. Gevolg is dat DRZ minder courante modellen in verkoop krijgt die weer minder opbrengen. Het gevaar bestaat dat de verkoopkosten niet meer gedekt zijn.

Met ingang van 1 juli 2010 verkoopt Domeinen geen geschoonde desk- en/of laptops meer, maar vernietigt deze via de shredder. Hiermee wordt bereikt dat:
- Geen desk- en/of laptops met overheidslogo's kunnen in handen komen van derden;
- Afval van de rijksoverheid wordt op een integere en milieuverantwoorde wijze verwerkt;
- Eenvoud van administratie: geen diverse tarieven voor het complexe schoningsproces maar verwerking/vernietiging tegen één prijs (per aangeleverde desk- of laptop slechts € 17,50).

> Voor de afstoot van de kleine datadragers zoals usb-sticks, memory cards, mobiele telefoons, e.d., coördineert Domeinen de gehele logistiek. Domeinen heeft hiertoe een speciale datacontainer ontwikkeld die zonder kosten geplaatst wordt en, indien vol, gewisseld wordt. De inhoud wordt vernietigd en gerecycled.

Uit: Informatieblad datavernietiging DRZ, 2010

Bij Domeinen is meer gedetailleerd navraag gedaan naar deze verwerkingsroute. Zo worden ict-hardware ook andere productsoorten door de shredder vernietigd: navigatieapparatuur, GSM's, USB sticks, filmcamera's, fototoestellen, tablets en CD-roms. Voor ict-apparatuur geldt dat het hele apparaat wordt geshredderd. Alleen bij serverkasten en kopieermachines met geheugen wordt de hardware gedemonteerd. Bij ontmanteling van de apparatuur die niet door de shredder gaat vindt verkoop plaats aan VIHB-vergunninghouders. Gerekend wordt met 3.000 manuren bij een volume van 30.000 systeemkasten.

De verwerkte aantallen HD-dragers (uitsplitsing naar type niet mogelijk):

2011	27.901
2012	50.575
2013	49.279

Solid state drives (SSD) hebben een andere verwerkingsroute vanwege het feit dat informatie kan worden achterhaald uit kleinere stukjes. Telefoon- en SSD-kaartjes worden met de hand verknipt, gaan in een perscontainer en gaan via een aparte vernietigingsstroom naar de verbrandingsoven. Zie hiervoor ook "Dataveiligheid, hoofdstuk 2.3".

Per desk- of laptop vraagt Domeinen € 17,50 voor complete ontzorging. In de (toelichting bij) de regeling materieelbeheer is aangegeven dat in het algemeen Domeinen intern een vast percentage van de gerealiseerde verkoopopbrengst (thans ca. 15%) doorberekent als kosten van afstoting aan het betrokken ministerie, tenzij die kosten aan de koper doorberekend kunnen worden (bijvoorbeeld bij de verkoop via veilingen).

<u>Datadragers</u>
Voor informatiedragers, zijnde papier, karton en overige informatiedragers is sinds 2010 een specifiek contract afgesloten. Op dit moment loopt ter opvolging van dit contract een aanbesteding voor de Rijksbrede afvoer en/of verwerking van informatiedragers en het verkopen van (rest) grondstoffen (vertrouwelijk papier en karton) ten behoeve van de Staat der Nederlanden. Voor de digitale informatiedragers zijn afgesloten inzamelmiddelen beschikbaar gesteld door de contractant. De hoeveelheid afgevoerde datadragers loopt terug, zoals blijkt uit onderstaand overzicht van (kilogrammen):

	Q1	Q2	Q3	Q4	Totaal (kg)
2011		16.585	2.382	783	19.750
2012	173.228	132.568	7.611	1.893	313.407
2013	3.590	2.649			

Op veel werkplekken is het al niet meer mogelijk om data te kopiëren naar losse datadragers.
In de nieuwe aanbesteding wordt uitgegaan van kostenloze verwerking van deze informatiedragers, en wordt uitgegaan van de duurzaamheidscriteria bij aanbesteding (http://www.rijksoverheid.nl/onderwerpen/aanbesteden/duurzaam-inkopen-door-overheden).
Tijdens de gesprekken is de indruk ontstaan dat de inzamelings- en verwerkingsroute zoals nu contractueel is vastgelegd niet bij iedereen (helemaal) bekend is.

2.2 Bevindingen verwerkingsroutes

Met een aantal inkooporganisaties binnen de rijksoverheid zijn gesprekken gevoerd om de praktijk bij afdanking van datadragende ict-apparatuur in beeld te krijgen. Daarbij ontstaat het beeld dat deze inkooporganisaties een grote mate van autonomie ervaren bij hun inkoop- en afvoerbeslissingen. Bij de keuze na aanbesteding kijken inkopers over het algemeen naar het totaalbeeld van de ict-apparatuur, van aankoop tot aan afdanking. Naast kosten ("verantwoord omgaan met belastinggeld") wordt ontzorging genoemd als belangrijke keuzefactor: is de leverancier in staat om verantwoord (informatieveiligheid) de inkopende overheidsorganisatie zoveel mogelijk, of liever helemaal, te ontlasten? De in de regeling materieelbeheer voorgeschreven route via Domeinen is blijkbaar niet vanzelfsprekend. De afgegeven signalen hierover zijn onder meer een hoge prijs, zelf inpakken/klaarzetten, zelf transport en daarbij horende overdrachtspapieren naar transporteur regelen, en geen zicht hebben op uiteindelijke bestemming van de apparatuur na verwerking bij Domeinen. Andere partijen bieden een volledige en gegarandeerde ontzorging, met certificaten van dataveiligheid na wissen en garanties over eindbestemmingen. Soms wordt apparatuur in eigen beheer gewist vóór afvoer. Overigens lijkt een en ander afhankelijk van de individuele inkoper: soms wordt al snel volstaan met opdrachtverlening naar een huidige leverancier vanwege de goede ervaringen, en/of wordt bij elke aanbesteding zelf gezocht naar mogelijke partijen.
Het lijkt erop dat bij aanbesteding geen heldere richtlijnen voor inkoop zijn vastgesteld of dat die niet voldoende zijn gecommuniceerd of worden gehandhaafd. De indruk is ontstaan dat van afgevoerde partijen zowel voor- als achteraf niet altijd melding wordt gedaan aan Domeinen. Mogelijk is zelfs de hele verwerkingsroute via Domeinen conform de regeling materieelbeheer bij (sommige) inkopers niet bekend. Ten aanzien van tablets en telefoons zijn inkopers niet op de hoogte van beleid/regelgeving met betrekking tot de verwerking. Gezien de toenemende aantallen en snelle vervanging is dit een zorgelijke ontwikkeling.
Melding werd gedaan van een grote aanbestedingsronde volgend jaar, wat een goede gelegenheid zou zijn om richtlijnen op te stellen cq aan te scherpen voor de inkoopprocedure.

Tot slot volgen drie huidige verwerkingsroutes zoals die in de gesprekken zijn genoemd naast de route via Domeinen. Benadrukt wordt dat formeel conform de regeling materieelbeheer Domeinen altijd moet zijn betrokken in de routing.

1. Onderscheid wordt gemaakt in data(drager)vernietiging, gericht op het onbruikbaar maken van de gegevensdrager, en dataverwijdering waarbij de informatie wordt verwijderd.
Datavernietiging gebeurt mechanisch (hydraulische schaar) of via een degausser. Na noteren van de unieke s/n nummers worden de HD's onder toezicht van een ingeschakelde partij vernietigd. Op verzoek worden foto's gemaakt van vernietigde

HDD's waarop het serienummer nog leesbaar is. De rapportage en verklaring van vernietiging worden verstuurd naar het ministerie.

Bij dataverwijdering worden data, conform richtlijnen van het Amerikaanse ministerie van Defensie en geaccordeerd door de AIVD, overschreven met afwisselende bitpatronen. De ingeschakelde marktpartij maakt gebruik van gecertificeerde Blancco software.
Na noteren van de unieke s/n nummers van alle ingenomen HD's worden de HD's via de beschreven methoden gewiped en worden rapportage en Blancco rapportages verstuurd naar het ministerie.

2. Een ingeschakelde marktpartij shreddert na wissen met gecertificeerde Blancco software de datadragers. Bij grotere partijen gebeurt dit op de rijksoverheidlocatie (geen transport- en overdrachtskosten), kleinere partijen worden getransporteerd naar een locatie van de marktpartij. Blancco rapportages worden door de marktpartij aangeboden.

3. De hardware gaat terug naar de leverancier (Fujitsu, HP, enz), en wordt naar wens behandeld. Op verzoek van de aanleverende partij kan apparatuur worden gerefurbished, vervangen of kan voor een andere oplossing worden gekozen binnen de Rijksbrede kaders en eisen.

2.3 Dataveiligheid

Voor het aspect dataveiligheid zijn gesprekken gevoerd met BZK, de AIVD-NBV, de RijksBVA en Blancco. Dataveiligheid is ook meegenomen in de gesprekken met de inkopers.
Uit deze gesprekken zijn een aantal aspecten naar voren gekomen die hieronder zijn weergegeven:

- Onderscheid soorten datadragers

Tijdens de verschillende gesprekken is naar voren gekomen dat de ontwikkelingen op ict-gebied leiden tot een aantal verschillende verwerkingsroutes. De route van de langer gangbare High
Density datadragers (HD) is inmiddels goed in beeld en uitgewerkt. Voor de relatief nieuwere Solid State Drives (SSD), met name te vinden in de huidige laptops, tablets, smartphones en usb-sticks, is de verwerkingsroute nog in ontwikkeling. Belangrijk verschil tussen HD en SSD is dat op SSD nog informatie te achterhalen is op kleine stukjes datadrager. Daarnaast is het lastiger SSD veilig te wissen vanwege de structuur en opbouw. Doordat een aantal soorten kleinere SSD (sticks, telefoonkaarten) te weinig waarde lijken te vertegenwoordigen om bewerkingen toe te passen die zouden kunnen leiden tot hergebruik worden deze veelal vernietigd via shredderen, magnetiseren, degaussen en/of verbranden.

- Ontwikkelingen programmatuur voor gecertificeerd wissen van data

Om hergebruik mogelijk te kunnen maken met als randvoorwaarde dataveiligheid is de verzekering vereist dat geen informatie op de datadragende apparatuur is terug te vinden. Door de AIVD is de software van Blancco gecertificeerd om informatie op HD tot en met de rubricering Stg Geheim gegarandeerd te verwijderen (https://www.aivd.nl/organisatie/eenheden/nationaal-bureau/artikel/goedgekeurde/#Overigebeveiliging). Blancco is doende om ook voor het hoogste rubriceringsniveau, en voor SSD software te ontwikkelen. De AIVD, en Blancco zelf, geven aan dat met de laatste versie van Blancco (Blancco 5) ook een groot aantal SSD's veilig kunnen worden gewist. Dit is echter vooralsnog afhankelijk

van merk en type SSD, en nog niet door de AIVD geëvalueerd (naar verwachting gebeurt dit in het eerste kwartaal van 2015). Blancco geeft aan deze programmatuur doorgaand te verbeteren, zodat steeds meer SSD's kunnen worden gewist. Blancco geeft ook aan het wissen van informatie met de rubricering Stg Zeer Geheim nader te onderzoeken.
Naast dat hier geen 100% veiligheid geboden wordt, wordt ook voorbij gegaan aan de menselijke handelingen die hiervoor nodig zijn, uit ervaring is reeds gebleken dat deze methode erg arbeidsintensief is, en de kosten die dat met zich meebrengen en de fout kans die verhoogd wordt in verband met menselijk handelen.

- Sommering rubriceringsniveau

Opgemerkt moet worden dat, door het sommeren van gerubriceerde informatie met een bepaald rubriceringsniveau op een datadrager, het rubriceringsniveau van deze datadrager kan worden verhoogd. Dit heeft te maken met het feit dat het afbreukrisico bepalend is voor de rubricering. Als voorbeeld geldt het verzamelen van gegevens die vallen onder de Wet bescherming persoonsgegevens, die an sich op een laag niveau zijn gerubriceerd maar die door het verzamelen van grote aantallen daarvan kunnen leiden tot een hoger rubriceringsniveau van de datadrager dan zou blijken uit de beoordeling van de individueel gerubriceerde informatie. Dit kan van belang zijn voor het gebruik van programmatuur voor gecertificeerd wissen.

- Veilig wissen van data in relatie tot rubricering

In principe moet bekend zijn als op een datadrager informatie met een verhoogd rubriceringsniveau zal/kan zijn gebruikt. De ministeries zijn, via hun CIO's (Chief Information Officers), CISO's (Chief Information Security Officers) en SSO's zelf verantwoordelijk voor de dataveiligheid bij ict-apparatuur. De ministeriële BVA dient er toezicht op te houden dat deze partijen hun rol en verantwoordelijkheid goed invullen.

Voor ict-apparatuur waarop geen gerubriceerde informatie is opgeslagen lijkt formatteren voldoende om zowel in- als extern hergebruik mogelijk te maken. Voor de rubriceringen tot en met Stg Confidentieel is gecertificeerd wissen van HD met software (vooralsnog is Blancco hiervoor de enige leverancier) toegestaan voor veilige dataverwijdering. Na gebruik van deze software is de apparatuur gereed voor zowel in- als extern hergebruik. Hergebruik van datadragende apparatuur tot en met Stg Confidentieel mag ook zonder wisbehandeling intern worden hergebruikt voor minimaal hetzelfde rubriceringsniveau, waarbij rekening moet worden gehouden met het "Need to know" principe.

Voor 'Stg. Geheim' en 'Stg. Zeer geheim' wordt vernietiging als enige veilige verwijderingsroute gezien. Voor hardware met de rubricering Stg Zeer geheim heerst altijd een aparte infrastructuur. Deze stroom zou bij afdanking derhalve relatief eenvoudig apart kunnen worden gehouden voor vernietiging. Overigens geeft de AIVD aan graag te zien dat de rubriceringen Stg Geheim en Zeer Geheim apart worden gehouden voor vernietiging (minder dan 5% van de gecertificeerd schoonbare datadragende ict-apparatuur). Apparatuur met de hoogste rubriceringen zijn altijd al aangemerkt als zodanig, en derhalve apart te houden van de overige apparatuur. Instructie voor personeel is hierbij essentieel. Ook wordt hierbij nog vermeld dat AIVD en het ministerie van Defensie gezien de gevoeligheid van hun informatie ieder over een eigen shredder beschikken. De procesvoering bij deze organisaties is niet onderzocht.

- Veiligheid huidige shredderverwerking

In het licht van de ontwikkelingen op het gebied van ict-apparatuur is tijdens het onderzoek nog de huidige verwerkingsroute (shredder) besproken. Diverse malen is naar voren gekomen dat de garantie op dataveiligheid van deze verwerkingsroute separaat onderzocht zou moeten worden. De huidige shredderverwerking bij Domeinen voldoet aan de richtlijnen van de AIVD die hiervoor zijn opgesteld. Gezien de ontwikkelingen richting SSD als opvolging van HD zou onderzoek zich moeten richten op de toekomstbestendigheid van de huidige shredderverwerking.

Samenvattend
Dataverwijdering van gerubriceerde informatie zoals hierboven beschreven gaat uit van inzicht in waar en door wie gerubriceerde informatie wordt gebruikt. Om dit inzichtelijk te houden om daarmee hergebruik van ict-apparatuur mogelijk te maken is essentieel, maar zal ook blijvend inzet en kosten meebrengen. Volgens de Rijksbrede kaders zou dit inzicht er moeten zijn. Tot en met het informatierubriceringsniveau Stg Confidentieel kan gecertificeerd schoonbare ict-apparatuur worden gewist met software, waarna externe afstoting kan plaatsvinden. In principe kan ook informatie met de rubricering Stg Geheim gecertificeerd worden gewist met software; door de AIVD wordt geadviseerd ict-apparatuur met zowel Stg Geheime als Stg Zeer Geheime informatie te vernietigen. Schoonbare Ict-apparatuur met lager gerubriceerde informatie kan worden gewist met gecertificeerde software en voor hergebruik worden aangeboden. In tabelvorm:

Rubriceringsniveau informatie	Gecertificeerd wissen mogelijk	Advies AIVD	% van totale hoeveelheid gecertificeerd schoonbare apparatuur
Stg. Zeer Geheim	Nee	Vernietigen	Geschat 2%; met veilige marge 5%
Stg. Geheim	Ja	Vernietigen	
Stg. Confidentieel	Ja	Wissen en hergebruik	Geschat 98%; met veilige marge 95%
Dep. Vertrouwelijk	Ja	Wissen en hergebruik	

2.4 Milieuaspecten

Met IenM en EZ zijn twee denklijnen besproken met betrekking tot dit project. Enerzijds de directe koppeling van milieu aan dit project (1), anderzijds de verbondenheid met de in gang gezette systeeminnovatie binnen de rijksoverheid (2).
Voor dit project (1) ziet IenM graag de denklijn van het principe van cascadering worden betrokken in de circulaire economie: alle componenten worden zo goed mogelijk benut, en als eerste worden de componenten gebruikt met de hoogste toegevoegde waarde. Het gaat dus om gebruik van, maar ook zo hoogwaardig mogelijk inzetten van die grondstoffen. Duidelijk moet zijn wat de uiteindelijke bestemming is van de materialen en grondstoffen. Aan de hand daarvan kan worden bezien welke verwerkingsroute het meeste bijdraagt aan een circulaire economie. De verwerkingsroute via de shredder van Domeinen levert computerscrap, en een deel van de ict-apparatuur (SSD-kaartjes) wordt afgevoerd naar een verbrandingsoven. De eindbestemming van de computerscrap na verwerking bij Sita wordt gerapporteerd aan Domeinen. Zoveel mogelijk wordt na geschikt maken voor hergebruik als grondstof gebruikt, zo zijn de Olympische medailles bijvoorbeeld vervaardigd uit e-waste.

Een aantal (markt)alternatieven geven gemotiveerd inzicht in het hergebruik en de eindbestemming van de ict-apparatuur en de materialen.

Met het ministerie van EZ is de grondstoffenstrategie en systeeminnovatie binnen de rijksoverheid (2) besproken. Grondstoffenstrategie richt zich met name op kritische en kwetsbare materialen: deze zijn in een database bij TNO, in samenwerking met het CBS, verzameld waarbij onder andere hoeveelheden, sectoren en gebruik zijn na te gaan. Grondstoffenmanagement koppelt beleid aan uitvoering. Daarnaast is Ict als productgroep in het rapport "Kansen voor een circulaire economie in Nederland (TNO, 2013)" opgenomen.
Binnen de rijksoverheid loopt het project "Systeeminnovatie in de bedrijfsvoering". In dit project worden een aantal systeeminnovaties onderzocht die leiden tot een betere sturing op het beleidsterrein en daarmee bijdragen aan versnelling van procedures, vermindering van bestuurlijke drukte, betere afbakening van taken en verantwoordelijkheden van overheden en scherpere toedeling van kosten. Onder meer het groene groei beleid wordt binnen dit project in een platform besproken. EZ zou graag ict-apparatuur hierbij inbrengen.

2.5 Financiële vergelijking

Tijdens het onderzoek zijn de financiële aspecten rond de verwerking van ict-apparatuur besproken met de inkopende organisaties en met Domeinen. Domeinen heeft aangegeven € 17,50 euro te rekenen per te verwijderen datadrager. Op korte termijn zal dit tarief inclusief transport zijn, dit wordt op dit moment verder uitgewerkt. Alle kosten voor de verwerking worden door Domeinen doorberekend in de stuksprijs.

Inkopers noemen € 35 als totaalkosten per eenheid bij afvoer via Domeinen (kosten inclusief handling, transport, eigendomsoverdracht), maar dit is niet hard onderbouwd. Zij geven aan dat andere marktpartijen minder (onder € 10) rekenen voor "volledige ontzorging". Daarbij wissen zij (deels) in eigen beheer, deels zit dit in de totaalprijs. Marktpartijen komen, bij voldoende grote partijen, op locatie binnen het terrein van de rijksoverheid voor verwerking.

Zoals in hoofdstuk 3 is aangegeven bieden marktpartijen naar eigen zeggen verwerking aan tegen een nultarief. Wat bij deze routes is inbegrepen is niet altijd helemaal doorzichtig. Een uitputtende vergelijking van kosten en opbrengsten tussen de route via Domeinen en de overige routes is lastig te maken. Wel lijkt het duidelijk dat de route via Domeinen de hoogste kosten (prijs plus handling) met zich meebrengen. Voordeel daarbij is dat de apparatuur in beheer blijft bij de rijksoverheid.

Zoals eerder aangegeven doorloopt niet alle afgedankte ict-apparatuur de route via Domeinen. De indruk is dat Domeinen ook niet op de hoogte wordt gebracht van afgevoerde partijen. Daardoor is ook onduidelijk hoe Domeinen de business case rond de eigen shredder heeft opgebouwd: wordt gerekend met ervaringscijfers van aantallen die door de shredder jaarlijks worden verwerkt? Of wordt uitgegaan van aantal fte's binnen de rijksoverheid en de vastgestelde vervangingstermijnen van ict-apparatuur?

De gegevens van een concrete verwerkingsaanbieding van een alternatieve marktpartij hebben financieel inzicht gegeven: daar waar bij de verwerkingsroute via Domeinen moet worden betaald per datadrager, is via een alternatieve route schijnbaar de mogelijkheid om opbrengsten te genereren voor de afstotende partij.

Deze indicatieve aanbieding heeft als basis gediend voor een marktconsultatie, waarin aan een aantal marktpartijen die verschillende verwerkingsroutes aanbieden is gevraagd concreet een voorstel te doen voor de verwerking van overtollige datadragende ict-apparatuur binnen de rijksoverheid. Hiertoe zijn deze partijen gevraagd een uniforme vragenlijst in te vullen, zodat objectieve vergelijking van de aanbiedingen mogelijk is. Ook aan de huidige verwerker Domeinen is deze vragenlijst voorgelegd. In de toelichting bij de vragenlijst voor deze marktconsultatie zijn de randvoorwaarden beschreven zoals die door de rijksoverheid zijn benoemd op het gebied van dataveiligheid, kosten en milieu. De rapportage van de marktconsultatie is vanwege de vertrouwelijkheid van de aangeleverde gegevens niet opgenomen in deze rapportage, maar is apart aan de stuurgroep voorgelegd. Een samenvatting van de marktconsultatie is geanonimiseerd opgenomen in hoofdstuk 3.6.

3 Alternatieve verwerkingsmethoden

Er zijn veel partijen in de markt die een service aanbieden voor het innemen van gebruikte Ict- apparatuur. Voorbeelden hiervan zijn hieronder verdeeld in vijf alternatieven. De huidige voorgeschreven route gaat via Domeinen, alwaar de apparatuur geshredderd wordt ten behoeve van recycling. Recycling is één van de hieronder genoemde alternatieven. Opvallend is dat over het algemeen gezien wordt dat cascadering voor de verwerking op basis van waarde van het materieel binnen bijna alle alternatieven voorkomt. Dit geldt niet voor het alternatief Recycling.

In de marktconsultatie, apart gerapporteerd, is voor een aantal verschillende verwerkingsmethodieken meer gedetailleerde informatie verzameld, zodat deze methoden overzichtelijk kunnen worden vergeleken.

3.1 Alternatief fabrikant

Diverse leveranciers (bijvoorbeeld Fujitsu Siemens, Dell, IBM, Apple) bieden terugname van afgedankte apparatuur aan. Deze bedrijven hebben programma's lopen voor het opnieuw inzetten van de apparatuur of het eventueel afdanken via recycling.

Gemak
Voordeel voor klant is ontzorging, en dat slechts met één partij wordt gewerkt. Inkoop van nieuwe apparatuur kan worden gecombineerd met laten afhalen van oude apparatuur.
Financieel
Gunstig. Oude apparatuur wordt gratis mee terug genomen.
Dataveiligheid
Onduidelijk. Deze wordt in de meeste gevallen gewist. Niet duidelijk hoe, met welke software. Bovendien wordt vertrouwen aan deze partijen gegeven, wat niet conform AIVD norm is.
Milieu
Lijkt gunstig. Afhankelijk van de economische waarde wordt hergebruik of recycling overwogen.

3.2 Alternatief zakelijke intermediair

Er zijn bedrijven die zich richten op de zakelijke markt. Deze bedrijven (bijvoorbeeld FEM systems en ARGO360) nemen afgedankte apparatuur in en leveren ICT infrastructuur en apparatuur waarbij waar mogelijk gebruik wordt gemaakt van deze hergebruikte spullen.

Gemak
Voordeel voor klant zijn dezelfde als bij de route 'Fabrikant': ontzorging, en dat slechts met één partij wordt gewerkt. Inkoop van nieuwe apparatuur kan worden gecombineerd met laten afhalen van oude apparatuur.
Financieel
Apparatuur wordt tegen lage kosten ingenomen. Doordat materieel wordt hergebruikt zijn de kosten voor aanschaffen van ICT over het algemeen lager. Aanbieders (bijvoorbeeld ARGO360) leveren soms ook lease contracten, met potentieel weer bijkomende voordelen.
Dataveiligheid

Data worden gewist met Blancco software. Dit wordt echter door deze partijen gedaan waardoor het niet voldoet aan de AIVD norm voor verwijdering van data van ICT apparatuur van de rijksoverheid.
Milieu
Gunstig. Afhankelijk van de economische waarde wordt hergebruik of recycling overwogen.

3.3 Alternatief charitatief

Er zijn veel organisaties (Recover-E, PC Donatie, IT Donations, Close the Gap, Techreturns, etc) die gratis afgedankte apparatuur komen ophalen. Drijfveer voor deze bedrijven en stichtingen is een charitatieve. Overeenkomsten zijn verder dat deze organisaties allemaal hergebruik en recycling aanbieden, afhankelijk van de economische waarde van de apparatuur. Grofweg zijn er twee stromingen: "product flows" en "money flows". Bij product flows wordt apparatuur in Nederland ingezameld en verspreid aan goede doelen wereldwijd, vooral naar Afrika. Veelal wordt een 'Track & Trace' gedaan opdat recycling (al dan niet in eigen land) van de uiteindelijk aldaar afgedankte apparatuur wordt gewaarborgd. Bij money flows gaat niet de apparatuur naar de goede doelen maar de opbrengsten van hergebruik en recycling in Nederland.

Gemak
Redelijk gemakkelijk. Organisatie komt de apparatuur ophalen.
Financieel
Gunstig. Apparatuur wordt kosteloos afgehaald.
Dataveiligheid
Data worden gewist met Blancco software. Dit wordt echter door deze partijen gedaan waardoor het niet voldoet aan de AIVD norm voor verwijdering van data van ICT apparatuur van de rijksoverheid.
Milieu
Gunstig. Afhankelijk van de economische waarde wordt hergebruik of recycling overwogen.

3.4 Alternatief recycling

Er zijn organisaties die betalen voor de waarde van afvalstromen. In sommige gevallen is dat B2C en wordt dat voor die doelgroep gecommuniceerd (Steeldeal). In andere gevallen betreft het afvalverwerkingsbedrijven die betreffende waardevolle afvalstromen recyclen (bedrijven als Sita, Van Gansewinkel). Feitelijk valt de praktijk van route Domeinen onder deze route.

Gemak
Redelijk gemakkelijk. Organisatie haalt het op, of het kan worden opgestuurd (B2C).
Financieel
Gunstig. Er wordt door deze partijen geld betaald voor de waarde van het materiaal.
Dataveiligheid
Onduidelijk, service van wissen wordt niet genoemd. Recycling betekent echter dat product tot materiaalstromen wordt teruggebracht, hetgeen data wissen tot gevolg heeft.
Milieu
Redelijk gunstig. Hergebruik krijgt echter een hogere waardering dan recycling.

3.5 Alternatief 'maatwerk'

Stichtingen ICT voor Morgen en ICT vanaf Morgen (kort: IvM) leveren geen standaard dienst, maar maatwerk op basis van de wens van de klant. Motivatie voor IvM zit in grondstofzekerheid voor ICT behoeften in de toekomst. Hergebruik van apparatuur en materialen nu, is van belang voor grondstofzekerheid voor ICT in de toekomst. De digitalisering van de samenleving en de noodzakelijke connectiviteit van iedereen is voor IvM een andere motivatie. Hergebruikte apparatuur wil IvM daarom graag inzetten voor mensen waarvoor deze connectiviteit lastiger te realiseren is.

Gemak
Niet eenvoudig. Deze route vergt dat de afdanker eerst nadenkt over wat er met de afgedankte apparatuur moet gebeuren. IvM kan wel helpen bij het bepalen van die visie.
Financieel
Potentieel Zeer gunstig. Opbrengsten gaan niet naar een charitatieve instelling, maar vloeien terug naar de afdanker.
Dataveiligheid
Data worden gewist met Blancco software. Dit wordt echter door deze partij gedaan waardoor het niet voldoet aan de AIVD norm voor verwijdering van data van ICT apparatuur van de rijksoverheid. Mogelijk kan in eigen beheer worden gewist.
Milieu
Gunstig. Afhankelijk van de economische waarde wordt hergebruik of recycling overwogen. Uitgangspunt is behoud van materialen.

3.6 Marktconsultatie

Zoals in hoofdstuk 2.5 al aangegeven is separaat een tweede deel van het onderzoek uitgevoerd, zijnde een marktconsultatie van een aantal aanbieders van verschillende verwerkingsroutes voor ict-apparatuur. Daarbij zijn deze marktpartijen middels een uniforme vragenlijst benaderd om concreet hun verwerkingsvoorstel in te vullen. Ook de huidige verwerker Domeinen is hiervoor benaderd. De randvoorwaarden zoals die binnen de rijksoverheid gelden zijn in de toelichting bij de vragenlijst uitgewerkt.

Uit de verzamelde informatie uit de marktconsultatie kan worden geconcludeerd dat er blijkbaar verwerkingsroutes zijn die op één of meer van de randvoorwaarden dataveiligheid, kosten en milieu beter scoren dan de huidige verwerkingsroute, vernietiging via de shredder en recycling van de scrap.

Bij de marktconsultatie is bij DRZ uitgegaan van de huidige verwerkingsmethodiek, de shredder. Op basis van de resultaten van het onderzoek gecertificeerd schonen en verkoop van 95% van de te schonen apparatuur, heeft DRZ een alternatieve businesscase voorgelegd. Hierbij schoont DRZ zelf en zorgt vervolgens voor verkoop van deze geschoonde apparatuur. Hieronder zijn de resultaten van de marktconsultatie geanonimiseerd weergegeven (DRZ wel identificeerbaar). Voor DRZ zijn in de tabel twee aanbiedingen weergegeven: het aanbod dat is gedaan vóór de marktconsultatie ('shredder') en het aanbod op basis van de businesscase waarin 95% van de hardware kan worden opgeschoond ('schonen').

Partij	Dataveiligheid		Financiën (negatief is kosten)	Milieu	
	HD	SSD		Milieu	Traceerbaar-heid
DRZ (shredder)	+	+	**- € 488.376,-**	--	++
DRZ (schonen) (*)	+	-	**€ 204.500,- (*)**	+ (*)	+ (*)
Aanbieder B	+	-	**€ 981.000,-**	+	++
Aanbieder C	+	-	**€ 7.368.900,-**	+	+/-
Aanbieder D	+	-	**€ 0,-**	+	++
Aanbieder E	-	-	Geen prijs geleverd	+	+/-
Aanbieder F	+	-	**€ 878.902,-**	+	+/-
Aanbieder G	+	-	**€ 182.100,-**	+/-	++

(*): De financiën en de milieuprestaties (milieu en traceerbaarheid) van de optie DRZ 'schonen' zijn afhankelijk van de organisatie die de apparatuur van DRZ uiteindelijk, na een formele aanbesteding, koopt. Voor de milieuprestaties en de financiële berekening van de businesscase 'schonen' is gerekend met de gemiddelde uitkomsten van de marktconsultatie (aanbieders B en F).

Met nadruk wordt erop gewezen dat het financiële deel van de marktconsultatie indicatief is; het betreft immers een verkennende marktconsultatie en geen formele aanbesteding.

Het verschil voor de Rijksoverheid tussen de shredder en schonen, gebaseerd op 30.000 stuks per jaar, is ca. € 692.000. De nieuwe businesscase van DRZ is wel gebaseerd op een aantal aannames, kan na een formele aanbesteding er anders uitzien, maar geeft op dit moment zeker een reëel beeld.

4 Conclusies en aanbevelingen

Uit het onderzoek kunnen een aantal conclusies worden getrokken en aanbevelingen worden gedaan. In dit hoofdstuk worden deze samengevat, waarna een voorstel voor vervolg is opgenomen.

4.1 Conclusies

- Er zijn heldere rijksbrede kaders voor veilig (her)gebruik van datadragers. Er zijn ook rijksbrede afspraken dat datadragers en ict-apparatuur centraal worden ingezameld via Domeinen.
- Via de regeling materieelbeheer is bepaald dat Domeinen altijd in de verwerkingsroute zit, maar dit is niet (altijd) bekend en wordt niet (altijd) gevolgd.
- Inkooporganisaties binnen de rijksoverheid lijken bij aanbesteding en opdrachtverlening een grote mate van autonomie te ervaren (deels binnen hun eigen ministerie).
- Er wordt een groot aantal hergebruik- en verwerkingsroutes gehanteerd voor afgedankte datadragende ict-apparatuur.
- Diverse overheidspartijen geven aan dat (markt)alternatieven goedkoper zijn en beter ontzorgen. Deze alternatieven bevestigen datavernietiging en verwerking op de eindbestemming met rapportages. De ervaringen hiermee hebben tot tevredenheid geleid.
- De AIVD steunt de lijn om alleen datadragers waarop informatie die gerubriceerd is met Stg Geheim of Zeer Geheim te vernietigen. Voorwaarde is wel is dat deze datadragers door de desbetreffende departementale ICT-organisaties worden gescheiden van andere datadragers met lagere rubricering, en dat het schoningsproces voldoet aan de eisen de AIVD daaraan stelt.
- Afgedankte ict-apparatuur (HD's en oudere laptops) waarop informatie tot en met de rubricering Stg Confidentieel aanwezig is (minimaal 95% van deze afgedankte apparatuur) kan worden gewist op een veilige manier waardoor het gereed is voor in- en externe verkoop. Hierdoor ontstaat voor de Rijksoverheid een dataveilige verwerkingsroute die financieel aantrekkelijk is en past in het streven naar een circulaire economie.
- SSD (sticks, tablets, smartphones, nieuwere laptops) zijn vooralsnog niet gecertificeerd schoonbaar; software hiervoor ligt bij de AIVD ter certificatie (naar verwachting 1^{e} kwartaal 2015). Ook voor apparatuur waarop informatie is verwerkt met de hoogste rubriceringen ligt software ter certificering bij de AIVD. Uitgangspunt blijft dat deze laatste apparatuur wordt vernietigd.
- De voorgestelde verwerkingsroute , grotendeels via schoning en hergebruik, leidt voor de Rijksoverheid tot een dataveilige, financieel aantrekkelijke oplossing die past in het streven naar een circulaire economie.

4.2 Aanbevelingen

Op basis van bovenstaande conclusies kunnen een aantal aanbevelingen worden voorgesteld:

- De centrale rol bij de verwerking van afgedankte datadragende ict-apparatuur blijft, conform de Regeling materieelbeheer, bij Domeinen. Hier komt de kennis van de markt en veilige afvoer samen.

- Bij de Ict-organisaties dient beter gestuurd te worden op naleving van de Regeling materieelbeheer. Zorg dat deze bij een ieder bekend is en gevolgd wordt.
- Laat Domeinen samen met de AIVD en de departementale ict-aanbieders het nieuwe afvoeren van ICT beschrijven, communiceer daar over en zorg voor controle.
- Zorg voor scheiding tussen apparatuur waarop informatie is verwerkt tot en met rubriceringsniveau 'Stg. Confidentieel' en apparatuur waarop informatie met hogere rubriceringsniveaus is verwerkt.
- Start een Europese aanbesteding voor de verwerking van gecertificeerd geschoonde ict-apparatuur (HD's).
- Zorg dat de randvoorwaarden dataveiligheid, kosten en milieu zoals beschreven in dit onderzoek (ook juridisch) kunnen worden gebruikt voor deze aanbesteding.
- De huidige verwerkingsroute bij Domeinen, de shredder, blijft de verwerkingsroute voor SSD en voor apparatuur waarop informatie met de hoogste rubriceringsniveaus is verwerkt, in elk geval tot software is gecertificeerd die ook deze apparatuur en SSD veilig kan schonen.
- Onderzoek (door Domeinen) of shredderen van steeds complexere schijven blijvend leidt tot 100% datavernietiging.
- Na certicering van schoningssoftware door de AIVD kunnen ook SSD gecertificeerd worden geschoond en hergebruikt.